A Novel Video Encryption Technique for Real Time applications

Padavala Yedukondalu[1], S. Madhavi Lakshmi[2]
[1]*PG scholar, Dept. of ECE, Helapuri Institute of Technology and Sciences, JNTU (Kakinada)*
[2]*Assisant Professor, Dept. of ECE, Helapuri Institute of Technology and Sciences, JNTU (Kakinada)*

Abstract- Various video encryption techniques are purposed to encrypt the videos and used for obtaining highly encrypted videos. In this paper, a method for encryption in video is taken place by using the Huffmann encryption algorithm. Instead of using the text or the images, the video encoding is taken place here. The video is converted into number of frames, which in turn converted to blocks used for encryption. The division of video resulted in images in turn this image is followed by encryption. The block cipher algorithm is used for converting frames to blocks. The DCT algorithm is used, because of its simplicity, efficient working syntax.

Index Terms— Deformation & formation Algorithm, Iframes, Video encryption.

I. INTRODUCTION

Because of quick improvement of different media advancements, more sight and sound information are created and transmitted in the restorative, business, and military fields, which might incorporate some delicate data which ought not to be gotten to by or must be halfway presented to the general clients. In this manner, security and protection has turned into a critical. The fundamental objective of cryptography is keeping information secure structure unapproved aggressors. In this manner information is scrambled through procedure of Encryption. The opposite of information encryption is information unscrambling. With advanced video transmission, encryption innovations are required that can shield computerized video from assaults amid transmission. Because of the enormous size of advanced recordings, they are generally transmitted in compacted organizations, for example, MPEG, or H.264/AVC (standard utilized for video pressure). Encryption of pictures and recordings are essential because of taking after reasons:

1. For averting undesirable survey of transmitted video, for instance from law authorization video observation being transferred back to a focal review focus.
2. To ensure the private multimedia messages that is traded over the remote or wired systems.
3. Video Encryption is useful in securing recordings utilized as a part of administrations such as video on interest (VOD), Video conferencing learning 4. For ensuring medicinal recordings which might contain private data of a patient from unapproved access by vindictive clients. This study depends on video encryption taking into account investigation of Deformation/Formation Algorithm which is valuable in securing different restorative recordings that contain private data of patients and requires sharing among different specialists that has a place with various department of hospital. The encryption and unscrambling of a plain content or a video stream should be possible in two ways:

A. Secret Key Encryption:

A single secret key can be used to encrypt and decrypt the video streams. Only the sender and the receiver have this key.

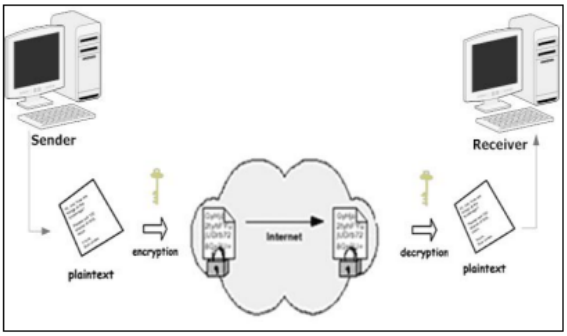

Fig.1 Symmetric key Algorithms [Ref. 1]

Basically, the security level of the symmetric keys encryption method is totally depends on how well the users keep the keys protected. If the key is known by

an intruder, then all data encrypted with that key can be decrypted. Most common algorithms in these categories are Data Encryption Standard (DES), Triple DES, and Advance Encryption.

B. Public key encryption:

There are two keys, one for encryption and the other for decryption. The public key, which is known for all senders, is used for encryption.

While the private key, which is owned only by the receivers, is used for decryption. [Ref. 2]. It is based on a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and solves the problem of secret key distribution by using two keys instead of a single key.

.

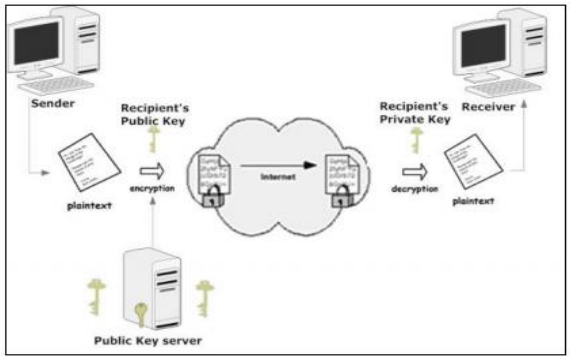

Fig.2 Asymmetric key Algorithms [Ref. 1]

A. Classification of video encryption methodologies

Since the mid-1990s many research efforts have been made to the development of specific video encryption algorithm. Fuhrt & Kirovski (2004) has given detailed overview of early video encryption methodologies. Later Fuwen Liu and Harmut (2010) classified encryption algorithms according to their association with video compression as compression independent encryption and joint compression and encryption methodologies.

A. Independent encryption: Encryption of video streams can occur before the compression or after the compression. This method has codec portability issue. When video is encrypted before compression it is codec portable but increases the data size. When video is encrypted after compression it is inherently not codec portable.

B. Joint compression and encryption: Encryption can also occur along with compression. This method is codec dependent and reduces overall processing time but it is less secure and may be computationally expensive. Video encryption methodologies can be classified into four categories.

A. Full encryption (Naïve approach):

The naïve approach is the most straight forward method where whole video data is encrypted. The video stream (bit sequence) is treated as text data, and every byte is encrypted using standard encryption algorithms like DES, RC5 or AES etc. This approach is supposedly the most secure as it is hard to break classical algorithms like 3DES or AES. This method is not suitable in real time video application since standard algorithms needs heavy computation; also, encrypting each and every byte will be a slow and expensive operation.

B. Selective encryption:

It is also called as partial encryption. It provides faster security because it encrypts only a selected portion of a bit stream. In this we will selectively encrypt the bytes within video frames that may contain sensitive information. This methodology is not encrypting each and every byte of video, thus, reduces computational power, produces less overhead and is much faster than full encryption.

C. Permutation based encryption:

The methods falling in this category use different permutation algorithms to scramble or encrypt the content of video.

The bytes within a frame are scrambled and permuted. For example in Zig-zag permutation [7], instead of mapping an 8X8 block to 1X64 vector in Zig-Zag order, it maps individual 8X8 block to 1X64 vector by using random permutation. The scrambling of each and every byte is not necessary. Permutation list can be a secret key to encrypt video contents. Scrambling offers fast distortion of video but is not considered as secure since all frames could be easily decrypted once the permutation list is figured out.

D. Perceptual encryption:

The requirement of the perceptual encryption is that quality of video is degraded by encryption to some extent i.e., the encrypted multimedia data are still partially perceptible after encryption. This method may find its application in entertainment industry where high quality of video is priced and will require an authorized access whereas low quality versions may be free to stimulate user to buy high quality version. The quality degradation of audio/visual content can be continuously controlled by a factor p.

Table1. Classification of video encryption methodologies

Full Encryption	Selective Encryption	Permutation based	Perceptual Encryption
Uses standard algorithms to encrypt every byte	Only selected bytes are encrypted	Permutation of DCT coefficients	Quality of video is degraded
Highly secure	Moderate secure	Not secure	Not secure
Needs heavy computation	Needs less computation	Needs less computation	Computations can be controlled
Slow	Fast	Very fast	Speed can be controlled

II. LITERATURE SURVEY

A. Methodology proposed by Qiao and Nahrstedt (1998): Scrambling:

This methodology is based on statistical analysis of compressed MPEG video stream. The basic idea is scrambling of bytes. Scrambling allows unauthorized users to have an arbitrarily degraded view of current video. In this method, the data is divided into two streams as odd and even numbered bytes and two streams are XORed forming the first part of the cipher. To construct the second part of the cipher, DES is performed over the even numbered byte streams. This method reduces the amount of data to be encrypted and is immune from known-plaintext attacks. [5]

B. Methodology proposed by Tang (1996): Zigzag permutation:

Tang embedded the encryption into the MPEG compression process. The ordering transformation coefficients are modified by using a random permutation matrix that act as secret key. In this method, I-frames of MPEG video undergo "Zig-Zag" reordering of 8X8 block to 1X64 vector. This method works in three main steps:

- Step1 generates a list of 64 permutation.
- Step2 splits 8X8 block by splitting the DC coefficient (8 bits) into two equal halves, 4 most significant bits are placed in DC coefficient and least significant bits as the last AC coefficient.
- Step3 applies random permutation to the split block.

This method is very fast but compromised security as it is vulnerable to known plaintext attack. Also, Zig-Zag permutation drastically increases the stream size. [6]

C. Methodology proposed by Wu and Kuo: MHT based algorithm.

They reconstructed the semantic content of image by fixing DC values at a fixed value and recovering AC coefficients. They proposed two schemes: multiple Huffman tables (MHTs) for the Huffman coder and multiple state index (MSI) for the QM arithmetic coder. First scheme encodes the input datastream using multiple Huffman tables. The table content and the order in which tables are used is used as secret key. Second scheme uses the idea to select 4 initial state indices and to use them in a secret and random order [11]. Major pitfalls of this methodology are:

- Decoding a Huffman coded bit stream without any knowledge about the Huffman coding tables would be very difficult.
- The basic MHT is vulnerable to known and chosen plaintext attacks.
- For MSI, It is very difficult to decode the bit stream without the knowledge of the state index used to initialize the QM coder.

III. PROPOSED SYSTEM

A. Huffman Codeword Permutation

It is a lightweight mpeg video encryption which incorporates encryption with MPEG compression in one step [12]. The primary goal of this methodology is to save computation time by taking the advantage of combining MPEG compression and data encryption and at the same time avoid decreasing video compression rate. In this permutation, Huffman codeword list is used as a secret key. During MPEG encoding, the encoder uses the secret key instead of standard Huffman codeword list. Since MPEG compression rate depends on Huffman codeword list, if we use an arbitrarily Huffman codeword list to encode the MPEG video, the compression rate may decrease.

To avoid affecting compression rate, it limits the permutation of Huffman codeword list (secret key) to those codewords which have the same length as the standard Huffman codeword. Second, it seems that not all of permutations of the Huffman codeword list can be used as an encryption keys. This makes key

generation difficult since a generated key has to be tested for validity before using.

B. Compression Logic based Random Permutation

The proposed algorithm is Compression logic based video encryption algorithm [13]. Instead of randomly permuting 8x8 coefficients of a single DCT block, the random permutation is applied to a number of permutation groups. Each permutation group contains the DCT coefficients of same frequency from every single block of a frame, regardless of I,P or B frame. Obviously, since each DCT block has 64 coefficients frequencies so that 64 permutation groups can be formed, the proposed algorithm runs random permutations on each of the permutation groups to encrypt a single video frame. After the random permutation the encrypted video data is compressed by standard RLE. It is also a selective algorithm since only a small number of permutation groups can be encrypted based on the requirements of confidentiality. It is reliable against brute force attacks due to a very large key space. It is secure against DCT vulnerability.

Proposed Deformation Algorithm

1) In this method, a video V_i is divided into I_1, I_2...I_n (where n=1, 2…..n) video frames such as frames are collected then take frame one by one.
2) Then, select two key Images namely K1, K2 as key frames for encryption and decryption process, so this key images can be send through secure channel.
3) Each frame has dimension of "w* h".
4) Let αi denotes any sorting permutation like quick sort, heap sort of Ii & α(Ii) is image with sorted pixels from 'Ii'.
5) Video stream is collection of still images & these images are refereed as I-frames.
6) Here, first frame is not encrypted & is transmitted through secure channel whereas
7) Second frame is xored with second key image, K2.Again the output is xored with sorted value of first frame.
8) The process is repeated for all frames till encrypted video sequences E1,E2….En are generated.

Formation Algorithm:

For decrypting the obtained sequence of encrypted video following steps are followed [Ref.5]:

1) Receive all frames of videos along with key images :K1,K2.
2) Each frame E1 is xored with first key image & again the output is xored with its previous frame i.e first frame initially. Then the output is xored with key image K2 to obtain first I-frame of video.
3) These steps are repeated for all the encrypted frames E1,E2..En (where n = 1,2…..n.).
4) Finally construct the final video (consisting of I1,I2……..In frames) by collecting all the frames.

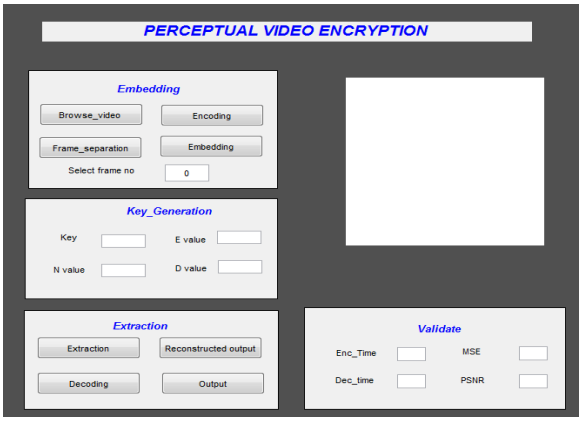

Fig.3 Experimental View

Fig.4 Encrypted View

Fig.5 Extracted View

IV. CONCLUSION

In this internet world nowadays, the security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently. From the above analysis; the following conclusions have been drawn: Amongst the two approaches: selective encryption takes less time as compared to full encryption. An encryption algorithm which maintains tradeoff among all parameters like visual degradation, speed, encoding/decoding time, compression friendliness, format compliance and cryptographic security and obtained good PSNR, MSE values.

REFERENCES

[1] M. Abomhara, Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.

[2] Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey", International Journal of Recent Trends in Engineering, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814.

[3] Daniel Socek, Spyros Magliveras,Dubravko Culibrk,Oge Marques, Hari Kalva, and Borko Furht, "Digital Video Encryption Algorithms Based on Correlation-Preserving Permutations", in EURASIP Journal on Information Security , Volume 2007,pp: 1-15.

[4] D.L. Gall, "MPEG: A video compression standard for multimedia applications," Communications of the ACM, Vol. 34, No. 4, pp. 46–58, 1991.

[5] Qiao L, Nahrstedt K., Comparison of MPEG encryption algorithms, International Journal of Computer and Graphics,1998;22(4);437-48.

[6] L.Tang, "For Encrypting and Decrypting MPEG Video Data Efficiently", in Proceedings of the Forth ACM International Multimedia Conference, 1996, pp. 219-230.

[7] Fadi Almasalha,Ashfaq Khokkar,Rogelio Hasimoto beltran, "Scalable Encryption of variable length Coded video Bit Streams",35th Annual IEEE conference on Local Com.

[8] Daniel Soek, Hari Kalva,Syyros S. Magliveras,"New Approaches to encryption and steganography for digital videos", MultimediaSystems,01 1007/s00530-007-0083-,@Springer-Verlag 2007.

[9] Knuth, D.E.: The art of computer programming, 2nd edn., vol. 3: Sorting and Searching, pp. 113–122. Addison–Wesley, Reading, MA (1998).

[10] S., Chen, G., Zheng, X.: Multimedia security handbook. Internet and Communications Series, vol. 4, chap. Chaos-Based Encryption for Digital Images and Videos, pp. 133–167. CRC Press, West Palm Beach (2004).

[11] Wu C-P, Kuo C-CJ, "Design of integrated multimedia compression and encryption systems". IEEE transaction on Multimedia (7)(5):828-39 ; October 2005